自由討論の要旨,付録、素最小原始根表 (実験整数論および組合せ理論と計算機)

AUTHOR(S):

一松, 信

CITATION:

一松, 信. 自由討論の要旨,付録、素最小原始根表 (実験整数論および組合せ理論と計算機). 数理解析研究所講究録 1977, 301: 143-148

ISSUE DATE:

1977-07

URL:

http://hdl.handle.net/2433/103801

数理解析研究所講究録
301巻 1977年 143-148

自由討論の要旨

10日午後の自由討論の時間には，前出山崎洋平の講演のほか，つぎのような話題が論ぜられた．

A. Millerの論文の紹介　　一松 信

B. 平方剰余のpatternについて（高橋秀俊の講演に対するコメント）　　内山三郎

C. 情報交換体制について　　田中穣 他

以下その要旨を記す．

A. Millerの論文の紹介

後藤英一より，下記の論文の指摘があった．

Gary L.Miller, Riemann's Hypothesis and Tests for Primality, Proc. of Seventh Annual ACM Symposium on the Theory of Computing, Albuquerque, N.M. 1975 May 5 - 7, p. 234-239.

正の整数nが素数か否かを判定するのに，正直に$\sqrt{n}$までの素数で順次割れば，$O(n^{0.5})$の手間を要する．Knuthの本には$O(n^{0.25})$でできる算法がある．この著者はまず$O(n^{0.134})$でできる算法を示し，ついでDirichletのL関数に対するRiemann予想の類似（$L(s,\chi)$の自明でない0点がすべて$\mathrm{Re}\,s=1/2$上にある；ERH）を仮

定して，$O(|n|^4 \log\log|n|)$ $(|n| = \lceil \log_2 n \rceil)$ でできる算法を与えた。

算法は(どちらも)つぎのとおりである：nが素数か？ ——

1° nが整数の累乗であるかを検査する。→ そうならNO.

2° (ある限界まで，$a = 2, 3, \cdots$について，次の検査を反復する：(nで定まる)

(i) $a \mid n$ か？ → そうならNO.

(ii) $a^{n-1} \equiv 1 \mod n$ か？ → そうでなければNO.

(iii) $(a^{(n-1)/2^k} \mod n - 1)$ とnとの最大公約数が，$k = 1, 2, \cdots$; $(n-1)/2^k$が奇数になるまで，すべてについて1か？ → そうでなければNO.

3° 以上の検査がすべて通れば，nは素数である。

限界は，$n = p_1^{v_1} \cdots p_m^{v_m}$ としたとき，$\lambda'(n) := (p_1 - 1), \cdots, (p_m - 1)$ のL.C.M. が$n-1$を割らないときは，最小の平方非剰余まで，割るときには，nを割る2つの素数p, qについて（$n = p^k$を除くために1°がいる），最小の，pに関するq次非剰余までで良く，その評価は前(の式)で与えられる。EHRはこれらの限界を示したAnkenyの定理に使われ，それ自体は直接にも証明できそうである。ただしOの係数を1としても，対数の4乗が0.134乗より小さくなるのは，(ほぼ)$n > 2^{56}$であって，実用価値は疑問かもしれない。

B. 平方剰余の pattern について

$k \geq 1$, $p > k$ を奇素数, $\varepsilon_i = \pm 1$ $(i = 0, 1, \cdots, k-1)$ を 2^k 個の pattern とする. $1 \leq a \leq p-k$ において, ε_i の列が与えられたとき

$$\left(\frac{a+i}{p}\right) = \varepsilon_i \qquad (i = 0, 1, \cdots, k-1)$$

であるような a の個数は,

$$p/2^k + O(k\sqrt{p})$$

であることが示される. もっと詳しく書けば, 剰余項の ( ) 内は

$$(k-1)\sqrt{p} + k$$

と書ける. ただし, $k = 1, 2$ については $O(1)$ とすべきである. このことは, 高橋秀俊教授の講演にあるとおり, ε_i の pattern がほぼ一様に起こることを示すといってよい.

証明は

$$\sum_{1 \leq a \leq p-k} \frac{1}{2^k} \prod_{i=0}^{k-1} \left(1 + \varepsilon_i \left(\frac{a+i}{p}\right)\right)$$

$$= \frac{1}{2^k} \sum_{a=1}^{p} \prod_{i=0}^{k-1} \left(1 + \varepsilon_i \left(\frac{a+i}{p}\right)\right) + O(k)$$

の項が, pattern があうときのみ 2^k, 他は 0 になることを

利用し，Weilの定理による評価

$$\left| \sum_{x \in GF(p)} \left(\frac{f(x)}{p} \right) \right| \leqq (\deg f - 1)\sqrt{p}$$

と組合せれば，示される．

C. 交換体制について

（田中）　近年は計算機が珍らしくなくなったせいもあり，生の計算データが発表されることが少なくなり，論文としては，たとえば妙にいねった統計結果という形で発表されることが多い．しかし加工された情報は，価値が低い．たしかに生の実験結果だけでは「数学」の論文にはなりにくいが，計算結果の情報交換体制が望まれる．

（中村）　数学パズルについても似た事情がある．数に関するものは，同人雑誌でとりあげられている．

これらを基にして，研究集会の活用，文献情報センターに集めて利用者の便をはかること，などの意見がだされた．

（なお6月17日の数学研連の小委員会にも，これをふまえて，計画中の「文献情報センター」の転務の一つとして，この種のデータ（論文になりにくい重要事実）の蒐集配布を考えてほしいという希望がのべられた．）

（文責　一松信）

付 録. 素最小原始根表

(一松 信)

岩波「数学辞典」第2版, p.955 に1000までの素数と原始根の表がある. 旧版も同じで, この表は昔の表をうつしたものであるため, 十進法計算時代を反映して, やたらに10(または−10)が多い. 多くの計算には, それ自体が素数であるような最小原始根のほうが便利であり, 以前からその点の御指摘をうけていた. 次回の改訂のおりには, この表および次の指数表を作り直す予定であるが, とりあえず計算機によって求めた素な最小原始根表のはじめのほうを掲げる. ここに示した範囲で, 「数学辞典」の表が最小な素数(下線のもの)の原始根を与えているのは, 僅か28個にすぎない. なおこの結果(の少なくともはじめのほう)は, プログラマブル電卓と暗算とで「検算」してある.

p	r	p	r	p	r	p	r
3	2	5	2	7	3	11	2
13	2	17	3	19	2	23	5
31	3	37	2	41	7	43	3
47	5	53	2	59	2	61	2
67	2	71	7	73	5	79	3

p	r	p	r	p	r	p	r
83	2	89	3	97	5	101	2
103	5	107	2	109	11	113	3
127	3	131	2	137	3	139	2
149	2	151	7	157	5	163	2
167	5	173	2	179	2	181	2
191	19	193	5	197	2	199	3
211	2	223	3	227	2	229	7
233	3	239	7	241	7	251	11
257	3	263	5	269	2	271	43
277	5	281	3	283	3	293	2
307	5	311	17	313	17	317	2
331	3	337	19	347	2	349	2
353	3	359	7	367	11	373	2
379	2	383	5	389	2	397	5
401	3	409	29	419	2	421	2
431	7	433	5	439	17	443	2
449	3	457	13	461	2	463	3
467	2	479	13	487	3	491	2
499	7	503	5	509	2	521	3
523	2	541	2	547	2	557	2

(以下回答)